UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,188	04/24/2001	Ulf Dahl	0104-0334P	2636

26161 7590 03/28/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
MAR 28 2006
Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/840,188
Filing Date: April 24, 2001
Appellant(s): DAHL, ULF

Thomas A. Brown
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 2, 2006 appealing from the Office action mailed July 22, 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: claims 48-54 and 86-92 are rejected under 101 as claiming a data structure without defining any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,751,949	THOMSON et al.	5-1998
5,148,481	ABRAHAM et al.	9-1992

Denning, D. E. "Field Encryption and Authentication" Advances in Cryptography, Proceedings of Crypto 83 (1983), pp 231-247

Pfleeger, C. P. Security in Computer, Chapter 8, Database Security, PTR Prentice Hall, (1989)

Gaskell et al. "Improved Security for Smart Card Use in DCE," February, 1995, Open Software Foundation, Request For Comments 71.0

Johansson et al. International Publication No. Wo 9515628, International Publication Date: June 8, 1995

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 18, 19, 21, 28, 29, 31, 33, 37, 41, 42, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 79, 80, 86 and 87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson et al. U.S. Patent No. 5,751,949 (hereinafter Thomson) in view of Denning "Field Encryption and Authentication" (hereinafter Denning).

As per claim 18, Thomson discloses a data processing method comprising:

a. maintaining a database containing a table of data in row and column format (fig. 2 and related text);

b. maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table (fig. 4 and related text); and

c. controlling access to the specified proper subset of data in the table according to the separately maintained information (figs. 5 and 6 and related text).

Thomson does not disclose at least a portion of the data being encrypted. Denning teaches a method of field encryption to secure information stored in tables having row and column format wherein each record is encrypted and stored using a distinct cryptographic key. Denning, page 233, section 2.2. The encryption technique ciphers each field of a record (a column in a table) with a distinct encryption key to prevent information from a record from being ascertained without the requisite key. As disclosed by Denning, enciphering at the field level enables a more selective means of hiding sensitive information (Denning, Introduction). It would be obvious to one of ordinary skill in the art at the time the invention was made for a portion of the data stored in a database containing a table of data in row and column format to be encrypted using distinct cryptographic keys for each record to establish a more secure database. Denning, page 233, sections 2.1 and 2.2. The aforementioned cover the limitations of claim 18.

As per claim 19, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, the step of controlling access comprises controlling access by a specified user or group of users. See Thomson, Figure 4, 'USER ID' and 'DEPT' columns.

As per claim 21, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, Thomson discloses a security table separate from the stored data. Thomson, col. 4, lines 44-54. Although Thomson does not expressly disclose making the security table inaccessible to a user seeking access to the data, means in the art to restrict access privileges to only tables relevant to a given user is a standard implementation in the art. For example, commercial databases, such as Oracle or Sybase, incorporate data dictionaries to define access privileges granted to a user on various schema objects (tables, views, indexes, synonyms). Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the separate table to be inaccessible to a user seeking access to the data since this enables access to security information on a need to know basis as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 21.

As per claim 28, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, the specified proper subset of data comprises a specified column of data. Thomson, fig. 4, 'USER ID' and figs. 5 and 6.

As per claim 29, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data. Thomson, fig. 4; Denning, page 233, section 2.2, 'Kij'.

As per claim 31, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). Thomson does not expressly teach the information for controlling access comprising information identifying an owner of the proper subset of data. However, data ownership is a typical attribute by which to define user access to data. For example, file access on commercial operation systems, such as UNIX, is restricted based on file ownership (user) and group membership. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made for the information controlling access to comprise information identifying an owner of the proper subset of data since this enables metadata of stored data to identify user access privileges and to maintain data privacy as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 31.

As per claim 33, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, the method further comprises:

d. receiving a request for access to a particular data element in the table, the particular data element containing encrypted data (Thomson, fig. 3, 'USER REQUEST'; Denning, page 233, section 2.2);

e. obtaining, from the separately maintained data, cryptographic information associated with a proper subset of data in the table, the proper subset containing the particular data element (Thomson, Figure 4; Denning, pages 238 and 239, section 2.4); and

f. decrypting the data in the particular data element using the cryptographic information (Denning, page 239, 1st full paragraph).

As per claim 37, Thomson covers a method as outlined above in the claim 33 rejection under 35 U.S.C. 103(a). In addition, the step of providing decrypted data from the particular data element further includes the step of providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request. Thomson, figs. 5 and 6; Denning, pg. 239, 1st full paragraph.

As per claims 41 and 42, Thomson covers a method as outlined above in the claim 21 and 37 rejections under 35 U.S.C. 103(a). In addition, Denning teaches encrypting data in a first column using first cryptographic information and encrypting data in a second column using second cryptographic information. Denning, pg. 233, section 2.2, 2nd sentence. Further, as argued in the claim 20 rejection above, user access restriction to security information is an obvious limitation.

As per claims 48 and 49, they are system claims corresponding to claim 21, and they do not teach or define above the information claimed in claim 21. Therefore, claims 48 and 49 are rejected as being unpatentable over Thomson in view of Denning for the same reasons set forth in the rejection of claim 21.

As per claim 56, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). In addition, Denning teaches the set of data as a collection of records having fields. Denning, Abstract.

As per claims 57, 59, 66-68, 70, 74 and 75, they are method claims corresponding to claims 18, 19, 21, 28, 29, 31, 33, 37 and 56, and they do not teach or define above the information claimed in claims 18, 19, 21, 28, 29, 31, 33, 37 and 56. Therefore, claims 57, 59, 66-68, 70, 74 and 75 are rejected as being unpatentable over Thomson in view of Denning for the same reasons set forth in the rejection of claims 18, 19, 21, 28, 29, 31, 33, 37 and 56.

As per claims 79, 80, 86 and 87, they are claims corresponding to claims 41, 42, 48 and 49, and they do not teach or define above the information claimed in claims 41, 42, 48 and 49. Therefore, claims 79, 80, 86 and 87 are rejected as being unpatentable over Thomson in view of Denning for the same reasons set forth in the rejection of claims 41, 42, 48 and 49.

As per claims 94-97, Thomson covers a method as outlined above in the claim 18, 41, 56 and 79 rejections under 35 U.S.C. 103(a). In addition, the step of controlling access to data in the first column comprises revealing unauthorized access to the data (pgs. 240-243, section 3, "Field Authentication"). It would be obvious to one of ordinary skill in the art at the time the invention was made for the method to reveal unauthorized access to data, since it is desirous to identify and prevent alteration of data by unauthorized users. Denning. Pg. 240, 3rd full paragraph.

As per claims 98 and 99, Thomson covers a system as outlined above in the claim 48, 86 and 94-97 rejections under 35 U.S.C. 103(a). In addition, the information for revealing unauthorized access to the database is stored outside the table (Denning, pg. 241, section 3.2 Solution, "Secret Key"; implied in the Denning reference is the storage of the key outside the table-all other elements in the table are either non-sensitive or encrypted).

Claims 20, 22, 43, 50, 58, 60, 81 and 88 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson in view of Denning, and further in view of Pfleeger Security in Computing (hereinafter Pfleeger).

As per claims 20 and 22, Thomson covers a method as outlined above in the claim 18 and 21 rejections under 35 U.S.C. 103(a). Thomson does not expressly disclose controlling access by a specified program or a group of programs. However, access control means to information stored in databases are conventionally known in the art to screen a user and/or a program. For example, Pfleeger teaches establishing access controls for a specific user or program. Pfleeger, pg. 306, 5th full paragraph 4th sentence. It would be obvious to one of ordinary skill in the art at the time the invention was made to control access by a specified program or group of programs since it is known in the art to establish database access control for a user or a program as taught by Pfleeger. Ibid. The aforementioned cover the limitations of claims 20 and 22.

As per claim 43, it is a method claim corresponding to claims 20, 22, 41 and 42, and it does not teach or define above the information claimed in claims 20, 22, 41 and 42. Therefore, claim 43 is rejected as being unpatentable over Thomson in view of Denning and Pfleeger for the same reasons set forth in the rejections of claims 20, 22, 41 and 42.

As per claim 50, it is a system claim corresponding to claim 22, and it does not teach or define above the information claimed in claim 22. Therefore, claim 50 is rejected as being unpatentable over Thomson in view of Denning and Pfleeger for the same reasons set forth in the rejection of claim 22.

As per claims 58 and 60, they are method claims corresponding to claims 20, 22 and 56, and they do not teach or define above the information claimed in claims 20, 22 and 56. Therefore, claims 58 and 60 are rejected as being unpatentable over Thomson in view of Denning and Pfleeger for the same reasons set forth in the rejections of claims 20, 22 and 56.

As per claims 81 and 88, they are claims corresponding to claims 43 and 50, and they do not teach or define above the information claimed in claims 43 and 50. Therefore, claims 81 and 88 are rejected as being unpatentable over Thomson in view of Denning and Pfleeger for the same reasons set forth in the rejections of claims 43 and 50.

Claims 23-27, 34-36, 38-40, 45-47, 52-54, 61-65, 71-73, 76-78, 83-85 and 90-92 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson in view of Denning, and further in view of Gaskell et al. “Improved Security for Smart Card Use in DCE” (hereinafter Gaskell).

As per claims 23-27, Thomson covers a method as outlined above in the claim 18 rejection under 35 U.S.C. 103(a). Thomson does not teach using a tamper-resistant hardware module to perform a cryptographic operation on the data, wherein at least a portion of the separately maintained information is located on the hardware module, the hardware module comprises a hardware security module and the hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card. Gaskell teaches incorporating smart cards into a data processing method to improve security by incorporating cryptographic authentication means, and decryption processes and keys stored within the smart devices. Gaskell, pg. 3, section 3.1. It would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate smart card technology within the method to provide more secure cryptographic authentication and secure communication between the user requesting access to a database and the database. Gaskell, section 1. The aforementioned cover the limitations of claims 23-27.

As per claims 34-36, they are method claims corresponding to claims 23-27 and 33, and they do not teach or define above the information claimed in claims 23-27 and 33. Therefore, claims 34-36 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 23-27 and 33.

As per claims 38-40, they are method claims corresponding to claims 23-27 and 37, and they do not teach or define above the information claimed in claims 23-27 and 37. Therefore, claims 38-40 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 23-27 and 37.

As per claims 45-47, they are method claims corresponding to claims 23-27 and 42, and they do not teach or define above the information claimed in claims 23-27 and 42. Therefore, claims 45-47 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 23-27 and 42.

As per claims 52-54, they are system claims corresponding to claims 23-27 and 48, and they do not teach or define above the information claimed in claims 23-27 and 48. Therefore, claims 52-54 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 23-27 and 48.

As per claims 61-65, 71-73 and 76-78, they are method claims corresponding to claims 23-27, 56, 70 and 75, and they do not teach or define above the information claimed in claims 23-27, 56, 70 and 75. Therefore, claims 61-65, 71-73 and 76-78 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 23-27, 56, 70 and 75.

As per claims 83-85 and 90-92, they are claims corresponding to claims 45-47 and 52-54, and they do not teach or define above the information claimed in claims 45-47 and 52-54. Therefore, claims 83-85 and 90-92 are rejected as being unpatentable over Thomson in view of Denning and Gaskell for the same reasons set forth in the rejections of claims 45-47 and 52-57.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson in view of Denning, and further in view of Johansson et al. International Publication Number WO 95/15628 (hereinafter Johansson).

As per claim 30, Thomson covers a method as outlined above in the claim 29 rejection under 35 U.S.C. 103(a). Thomson does not disclose the information used in encrypting or decrypting data comprises information identifying a way of encrypting or decrypting data in the proper subset of data. Johansson teaches storing information identifying a way of encrypting or decrypting data for given stored information. Johansson, pg. 6, lines 7-8; page 12, lines 9-14. It would be obvious to one of ordinary skill in the art at the time the invention was made for the information used in encrypting or decrypting data comprising information identifying a way of encrypting or decrypting data in the proper subset of data to ensure correct cryptographic processing wherein encrypted data is re-encrypted using an encryption algorithm distinct from the original encryption algorithm. Johansson, pg. 2, last paragraph-page 3, first paragraph. The aforementioned cover the limitations of claim 30.

Claims 32, 44, 51, 69, 82 and 89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomson in view of Denning, and further in view of Abraham et al. U.S. Patent No. 5,148,481 (hereinafter Abraham).

As per claim 32 and 44, Thomson covers a method as outlined above in the claim 18 and 41 rejections under 35 U.S.C. 103(a). Thomson does not expressly disclose the first and second information are stored, in encrypted form, outside of the table. Abraham teaches storing encrypted key values for encryption/decryption algorithms in a plurality of devices including cryptographic accelerators and smart cards. Abraham, col. 7, lines 42-50. It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second information to be stored, in encrypted form, outside of the table to secure cryptographic information used to secure data as known to one of ordinary skill in the art and as taught by Abraham. Ibid. The aforementioned cover the limitations of claims 32 and 44.

As per claim 51, it is a system claim corresponding to claims 32 and 48, and it does not teach or define above the information claimed in claims 32 and 48. Therefore, claim 51 is rejected as being unpatentable over Thomson in view of Denning and Abraham for the same reasons set forth in the rejections of claims 32 and 48.

As per claim 69, it is a method claim corresponding to claims 32 and 56, and it does not teach or define above the information claimed in claims 32 and 56. Therefore, claim 69 is rejected as being unpatentable over Thomson in view of Denning and Abraham for the same reasons set forth in the rejections of claims 32 and 56.

As per claims 82 and 89, they are claims corresponding to claims 44 and 51, and they do not teach or define above the information claimed in claims 44 and 51. Therefore, claims 82 and 89 are rejected as being unpatentable over Thomson in view of Denning and Abraham for the same reasons set forth in the rejections of claims 44 and 51.

NEW GROUND(S) OF REJECTION

Claims 86-92 and 48-54 are rejected under 101 as claiming a data structure that does not define any structural and functional interrelationships between a database and other claimed aspects of the invention which permit the data structure's functionality to be realized. The claims define in substance a database having a table with at least one column of encrypted data, and information for controlling access to at least one column wherein the information includes cryptographic information associated with the encrypted column of data. However, no functional interrelationship between the data 68 structure and the information is defined. The portion of the claim "for controlling access to at least one column of data" merely describes an intended use and does not narrow the scope of the claim. Also, the portion of the claim "the information including cryptographic information associated with the encrypted column of data" does not disclose any functional interrelationship, only an association. For these reasons, the subject matter of these claims are deemed to be nonstatutory.

(10) Response to Argument

The Examiner summarizes the various points raised by the Appellant and addresses the replies individually.

Appellant argues in substance:

in reference to claims 18 and 56:

(A) on pgs. 10-13 of the Brief, Appellant argues that neither the Thomson reference nor the Denning reference disclose "maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table;" specifically,

(A1) in regards to the Thomson art, Appellant argues that because the security table in Thomson restricts access to the entire table, the security table does not include "information for controlling access to a specified proper subset of data," and hence, that Thomson does not teach or suggest "maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table"; and

(A2) in regards to the Denning art, Appellant argues that the master key used to generate the field keys "is not information associated with a proper subset of data in the table-it is associated with the entire table," and, although Appellant concedes that field keys "may be viewed as "information for controlling access to a specified proper subset,"" Appellant argues that the "field keys are calculated on an as-needed basis, not "maintained,"" and hence the limitations are not taught by Denning;

in reference to claims 32, 44, 51, 69, 82 and 89:

(B) on pgs. 13-15 of the Brief, Appellant argues that the prior art Thomson, Denning and Abraham reference fails to teach or suggest the additional limitation that the information for securely accessing portions of the table is encrypted;

in reference to claims 23-27, 34-36, 38-40, 45-47, 52-54, 61-65, 71-73, 76-78, 83-85 and 90-92:

(C) on pgs. 15-19 of the Brief, Appellant argues that the prior art of Thomson, Denning and Gaskell do not teach the limitations of the claims, in particular Appellant argues in substance the following two points: 1) because Gaskell teaches using a smart card to authenticate to an entire system, and not a proper subset of data, Gaskell does not disclose the additional limitations of the dependent claims and 2) because Gaskell teaches using the smart card to perform a cryptographic operation on a Ticket-granting ticket and not on data in a table, Gaskell does not disclose the additional limitations of the dependent claims;

in reference to claims 41, 42, 79, 80, 95, and 97:

(D) on pgs. 7-10 of the Brief, Appellant argues that (D1) Denning fails to disclose storing cryptographic information outside the table and (D2) Denning fails to disclose storing second cryptographic information;

in reference to claims 18, 19, 21, 28, 29, 31, 33, 37, 48, 49, 56, 57, 59, 66-68, 70, 74, 75, 86, 87, 94, 96, 98 and 99:

(E) on pgs. 10-11, Appellant argues that Denning does not disclose the limitation of information stored outside the table including cryptographic information associated with an encrypted column of data.

In reply to Appellant's argument (A1), Appellant's argument does not fully consider the role of the security table in relation to the access views. In particular, Thomson discloses the following:

> The server computer includes relational database software for creating and maintaining tables, including the server table, and views defining subsets of the tables. **A security table is stored in the computer for identifying authorized user access to preselected rows of the server table for pre-identified users.** An access view is stored in the computer for automatically joining the security table to the preselected rows thereof based on the security table. (col. 2:18-26 [emphasis added])
>
> Accordingly, in order to readily implement row security of the TABLE1 a single Security TABLE-S is created by the administrator and stored in the server computer 12 for [sic] Identifying

> authorized user access to preselected rows of the server TABLE1 for pre-identified users as illustrated in FIG. 3. In addition, a suitable access view, such as first VIEW1 is created by the administrator and is also stored in the server computer 12 for automatically joining the Security TABLE-S and the corresponding server table such as TABLE1 to **limit user access to the server table to solely preselected rows** thereof based on the Security TABLE-S. (col. 4:15-26 [emphasis added])

As disclosed by Thomson, the security table joined with a particular access view meets this limitation, i.e. that the security table joined with the particular access view controls access to a specified proper subset. Therefore, since the security table joined with the access views are separate entities from the server tables, and further, these separate entities maintain information to restrict access to preselected rows of the server table, Thomson discloses "maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table."

<u>In reply to Appellant's argument (A2)</u>, there are two issues with Appellant's argument. First, the argument is contingent on the assumption that any information associated with the entire table is separate and distinct from information associated with a proper subset of the table. This is not a proper measurement of the breath of the limitation. Case in point, if element {a} in set A, is mapped to every element in set B, then element {a} is necessarily mapped to any proper subset of set B. In the case of the claim limitation in question, a key that controls access to the entire table, necessarily controls access to a specified proper subset of data in the table. Hence, the master key

is information that is maintained "for controlling access to a specified proper subset of data in the table." Second, Appellant's argument that because the field keys are "calculated", they are not "maintained," undermines the examination directive for the broadest reasonable interpretation of the claims. In this case, what constitutes being "maintained?" Since there is no special meaning attributed to the term "maintaining" in the Specification, under the plain meaning of the word, "maintaining," is defined as: providing for, supporting or keeping in existence or sustaining. (see www.dictionary.com, Webster's Dictionary or any equivalent) So in the context of the claim, "maintaining ... information for controlling access to a specified proper subset of data in the table" is equivalent to: providing for, supporting or keeping in existence or sustaining information for controlling access to a specified proper subset of data in the table. Given this breath, "calculating" keys falls under the umbrella of "maintaining" information.

In reply to Appellant's argument (B), Examiner respectfully disagrees. As cited in the rejections under Grounds of Rejections and further elaborated both above and below, Thomson and Denning clearly disclose key information that encrypts portions of the data table, the key information being maintained separate from the data table. Moreover, Abraham discloses storing any keys used for cryptographic operations in encrypted form, and storing these keys in a variety of places. The portion of Abraham cited in the Final action mailed on July 22, 2005 is column 7, lines 42-50, which states:

> The keys used for generation of message authentication codes, encrypting other keys, and ordinary encryption and decryption tasks can be stored in many places in the secure network. Keys are stored on PC disk memory in encrypted form, encrypted under the master key of one of the security devices. [sic] cryptographic adapter 29, card reader 17, or IC card 19. Keys are also stored in the nonvolatile memories of cryptographic adapter 29, card reader 17, and IC card 19.

Since encrypted key values maintains the privacy of the key values as known to one of ordinary skill in the art, Thomson, Denning and Abraham teach or suggest the limitations of claims.

In reply to Appellant's Argument (C), Appellant makes the argument against the references individually. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). As outlined in the rejection, Thomson and Denning disclose restricting access to a proper subset of a table using encrypting keys that are not stored in the table. Gaskell discloses using smart cards to store cryptographic keys and performing cryptographic operations with these keys on data received by the card. Since the advantages of using a smart card for cryptographic operations is notoriously well known, Thomson, Denning and Gaskell teach or suggest the limitations of the claims.

In reply to Appellant's argument (D1), the following "proof by contradiction" is demonstrated to show that the Denning reference does in fact teach or suggest that the cryptographic information is not stored in the data table.

Denning teaches using a distinct cryptographic key for each data element of a table to encrypt the elements of the table. In particular, Denning discloses the following construction:

> Let Kij denote the element key for record i, field j, Xij is an element in the table in record i and field j, then for any value in the table, Xij is encrypted as Cij = Ekij(Xij) (section 2.2 "Solution", pg. 233: "Our solution is simply to use a distinct cryptographic key for each data element; that is, for each record, and for each field within a record. Letting Kij denote the element key for record i, field j, the value Xij is then encrypted as Cij = Ekij(Xij).")
>
> Further, Kij = g(Ri, Fj, K), where g is a key generating function, and K is the secret database key (the Master key) (section 2.3, pg. 234: "An element key Kij is defined as Kij = g(Ri, Fj, K), where g is a key generating function, and K is the secret database key.")

Let's assume that the cryptographic information of Denning is stored in the table as Appellant has proposed as a possible condition of Denning.

Proposition 1: *the master key is encrypted.* Since any sensitive values of the table are accessible, all sensitive values must be encrypted. The master key is a sensitive value. Therefore, the master key is encrypted.

Proposition 2: *the master key is encrypted using the key values not defined by Denning.* The master key is either encrypted using the key values defined by Denning or key values not defined by Denning. Since all the keys defined by Denning is either the master key or generated using the master key, the master key cannot be used to encrypt itself without losing the viability of the master key; hence, the master key is encrypted using a key value not defined by Denning. Moreover, this key value not defined by Denning is not generated using the master key. (for reasons just disclosed)

Then there exits a key value not defined by Denning that is not generated using the master key, (lets call this key value Kxy), and this key is used to encrypt the master key to generate the encrypted value Cij = Ekxy(Xij). But this contradicts Denning's originally disclosure that for any value (Xij) of the table, that value is encrypted as Cij = Ekij(Xij). In other words, in order to assume that the master key is stored in the data table, the solution of Denning would require modification. On the other hand, storing the master key separate from the table does not require invalidating the conditions set forth by Denning. Therefore, the master key is not stored as an encrypted value using a key not disclosed by Denning, and hence, the master key is not stored in the table.

In reply to Appellant's argument (D2). Appellant fails to take in account the breath of the limitation. The limitation of the claim in question is as follows: "encrypting data in a first column using first cryptographic information; encrypting data in a second column using second cryptographic information; storing first and second cryptographic information outside the table." The Denning reference is found to cover the limitations for the following reasons. As argued above, the master key is not stored in the table. Since the master key generates all other cryptographic keys, it must be stored outside the table. The master key is used to encrypt data in a first column. Hence, the master key is first cryptographic information. The master key is used to encrypt data in a second column. Hence, the master key is second cryptographic information. Therefore, the first and second cryptographic information is stored outside the table.

Furthermore, the field keys disclosed by Denning also cover the limitation "encrypting data in a first column using first cryptographic information; encrypting data in a second column using second cryptographic information; storing first and second cryptographic information outside the table." Since each field key enciphers only a specific data element within the table, the limitation "encrypting data in a first column using first cryptographic information; encrypting data in a second column using second cryptographic information" is met. Further, the field keys are generated prior to being used to encrypt and decrypt the data elements. Denning discloses using these field keys in ciphering methods such as DES (pg. 240, 1st paragraph). Since DES operates on the key values separately from the data values (DES is a block cipher having multiple rounds; for each round of DES, a shift operation then a compression permutation is performed on the key before being XORed with the data), any generated key used by a DES cipher requires the temporary buffer of key values before being used to encipher the data. Hence, the limitation, "storing first and second cryptographic information outside the table" is also met.

Finally, Apellant's argument (E), is substantially similar to the arguments (A2) and (D), which have been addressed above.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

This examiner's answer contains a new ground of rejection set forth in section **(9)** above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

Respectfully submitted,

Jung Kim

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

James Dwyer

Conferees:

Gilberto Barron

Kambiz Zand

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

James Dwyer
Director TC 2100